ANÁLISIS DE VULNERABILIDAD EN CONTRASEÑAS DE CORREOS ELECTRÓNICOS.

William Alexander Caicedo Olaya
william.caicedo01@usc.edu.co

Brayan Esteban Rojas Cardona
brayan.rojas01@usc.edu.co

Facultad de Ingeniería

Ingeniería de sistemas

2024

Diplomado en ciberseguridad

ANÁLISIS DE VULNERABILIDAD EN CONTRASEÑAS DE CORREOS ELECTRÓNICOS.

William Alexander Caicedo Olaya (1)
william.caicedo01@usc.edu.co

Brayan Esteban Rojas Cardona (1)
brayan.rojas01@usc.edu.co

Alejandro Esteban Marcus (2)

alejandro.marcus00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de sistemas (1)
Universidad Santiago de Cali, Facultad de Ingeniería (2)

Resumen

En la era digital, la seguridad de las contraseñas ha cobrado una importancia crítica debido al aumento en la dependencia de plataformas en línea para la gestión de información tanto personal como profesional. Con la creciente conectividad y el intercambio masivo de datos sensibles a través de correos electrónicos, las vulnerabilidades relacionadas con las contraseñas han aumentado considerablemente. Contraseñas débiles, la reutilización de credenciales y ataques como el phishing y cracking exponen tanto a individuos como a organizaciones al riesgo de accesos no autorizados y explotación de información.

Este estudio se enfoca en analizar las contraseñas vulnerables en correos electrónicos, examinando los casos más comunes de malas prácticas en su gestión. Las amenazas relacionadas con las contraseñas no solo afectan a los usuarios individuales, sino que también comprometen infraestructuras críticas y servicios esenciales, lo que magnifica el impacto de posibles brechas de seguridad. Entre las estrategias propuestas, destacan la autenticación multifactorial, el uso de contraseñas generadas automáticamente mediante algoritmos, y la implementación de gestores de contraseñas para crear credenciales complejas y seguras.

La investigación revela patrones de vulnerabilidad que refuerzan la necesidad urgente de mejorar las prácticas de seguridad en correos electrónicos. Además, se subraya la importancia de un enfoque integral de ciberseguridad, en el cual tanto los usuarios como los desarrolladores de tecnología compartan la responsabilidad de fomentar una cultura de seguridad que proteja la privacidad y mantenga la confianza en las plataformas digitales. Una adecuada protección de contraseñas es clave para garantizar la integridad de los datos.

Palabras clave: Autenticación de usuarios, ciberseguridad, brechas de seguridad, contraseñas vulnerables, seguridad de la información

Abstract

In the digital age, password security has become critically important due to the increased reliance on online platforms for both personal and professional information management. With increasing connectivity and the massive sharing of sensitive data via email, password-related vulnerabilities have increased significantly. Weak passwords, reuse of credentials and attacks such as phishing and cracking expose both individuals and organizations to the risk of unauthorized access and data exploitation.

This study focuses on the analysis of vulnerable passwords in emails, examining the most common cases of poor password management practices. Password-related threats not only affect individual users, but also compromise critical infrastructures and essential services, magnifying the impact of potential security breaches. Among the strategies proposed are multi-factor authentication, the use of automatically generated passwords using algorithms, and the implementation of password managers to create complex and secure credentials.

The research reveals patterns of vulnerability that reinforce the urgent need to improve email security practices. It also underscores the importance of a comprehensive approach to cybersecurity, in which both users and technology developers share responsibility for fostering a culture of security that protects privacy and maintains trust in digital platforms. Proper password protection is key to ensuring data integrity.

Keywords: User authentication, cybersecurity, security breaches, vulnerable passwords, information security

1. INTRODUCCIÓN

Las contraseñas son una de las tecnologías de seguridad más comunes que la gente usa a diario. Elegir una nueva contraseña es una decisión de seguridad que puede tener consecuencias importantes para los usuarios finales. Las contraseñas pueden ser largas y complejas, priorizando los aspectos centrados en la seguridad de una contraseña. También pueden ser simples (fáciles de crear, recordar y usar), lo que prioriza los aspectos de usabilidad de la contraseña. La disyuntiva entre la seguridad de la contraseña y la usabilidad representa restricciones en pugna que dan forma a la creación y el uso de contraseñas. (Wash & Rader, 2021) Es sorprendente que la cantidad de contraseñas que cada uno de nosotros debe utilizar siga aumentando año tras año, a pesar de que los usuarios las califican regularmente como un gran inconveniente y los profesionales de la seguridad citan las contraseñas débiles o reutilizadas como algunas de las vulnerabilidades de seguridad más comúnmente explotadas. (Aebischer et al., 2020). A pesar de estos avances, la vulnerabilidad de las contraseñas sigue siendo un problema significativo en la era digital actual, caracterizada por una creciente dependencia de plataformas en línea y servicios digitales en todos los ámbitos de la sociedad (Maldonado et al., 2022).

La seguridad de la información ha ganado prioridad en la era digital, donde la creciente dependencia de plataformas en línea y servicios digitales resalta la importancia de proteger sistemas, redes y datos contra amenazas cibernéticas. Además, la autenticación de usuarios a través de contraseñas es uno de los elementos clave de la ciberseguridad, junto con otras prácticas y medidas diseñadas para prevenir accesos no autorizados y proteger la integridad de la información (Wang et al., 2024).

En este contexto, la autenticación de usuarios sigue siendo uno de los pilares fundamentales de la ciberseguridad. Sin embargo, persiste el uso generalizado de contraseñas débiles y fácilmente vulnerables, lo que expone a individuos y organizaciones a riesgos de acceso no autorizado y explotación de datos sensibles (Zimmermann & Gerber, 2020). Por ejemplo, investigaciones como las de Morris y Thompson han demostrado que aproximadamente el 30 % de 3,000 contraseñas pueden ser comprometidas mediante un ataque de diccionario con 250,000 palabras conocidas, y un 86 % puede ser vulnerado con ataques de fuerza bruta.

La persistencia de prácticas de seguridad deficientes, como el uso de contraseñas débiles y la reutilización de las mismas en múltiples cuentas, sigue siendo una preocupación crítica. Estas prácticas no solo facilitan los ataques cibernéticos, sino que también subrayan una falta generalizada de conciencia sobre la importancia de elegir contraseñas robustas y gestionarlas adecuadamente (Wash & Rader, 2021; Ezugwu et al., 2023). Este problema se ve agravado por la preferencia de los usuarios por la simplicidad y la conveniencia sobre la seguridad, lo que a menudo resulta en un falso sentido de seguridad y un entorno favorable para el acceso no autorizado a datos confidenciales.

En este sentido, la creciente dependencia de la sociedad actual en el entorno digital ha propiciado un aumento exponencial de las amenazas cibernéticas (Woods & Siponen, 2024). Entre los principales factores que contribuyen a la vulnerabilidad del sistema se encuentran la debilidad en la seguridad de las contraseñas y la gestión inadecuada de los usuarios finales. En relación con la Seguridad Ciudadana, los ciberataques en Colombia impactan negativamente el sector económico (entre muchos otros). De hecho, cerca del 43% de las empresas colombianas no están preparadas para enfrentar ciberataques, pues solo en 2015 Colombia registró pérdidas por cerca de 1 billón de dólares por ciberataques (Castro, 2022).

A pesar de la disponibilidad de soluciones alternativas, como administradores de contraseñas y autenticación biométrica,

la adopción de estas tecnologías sigue siendo limitada. Estudios han demostrado que, aunque los administradores de contraseñas existen desde la década de 1990, su uso sigue siendo bajo debido a preocupaciones sobre su seguridad percibida y su facilidad de uso (Gaw et al., 2019). Del mismo modo, la biometría se utiliza cada vez más para la autenticación debido a su singularidad, universalidad y accesibilidad. (Chhibbar et al., 2024), en la actualidad, encontrar sistemas de autenticación multifactor es común, en especial en los sitios web de las entidades financieras y las que se dedican al comercio electrónico (Mendoza et al., 2020).

Por lo tanto, a pesar de las limitaciones y desafíos asociados con las contraseñas, siguen siendo el mecanismo de autenticación más popular y ampliamente utilizado (Atzori et al., 2024). La investigación en este campo se ha centrado en mejorar la memorabilidad de las contraseñas sin comprometer su seguridad, una tarea que, aunque ardua y a menudo considerada imposible, sigue siendo crucial para la protección de la información en la era digital.

En el escenario actual de la ciberseguridad en Colombia, surge una preocupación significativa en torno a la magnitud de las amenazas digitales que enfrentamos. Un indicador impactante de esta realidad es el reciente registro de nada menos que 7 billones de intentos de ciberataques. Esta cifra evidencia la falta de ciberseguridad en Colombia.

En cuanto al Estado colombiano uno de los últimos datos recientes son del registrador Alexander Rocha el cual reveló que, durante las elecciones legislativas, la página web de la Registraduría Nacional enfrentó un asombroso total de 400.000 ataques en tan solo una semana (Castro, 2022). Esta cifra resalta la vulnerabilidad significativa a la que se enfrenta la infraestructura digital gubernamental. En cuanto a las otras principales entidades del Estado Colombiano, se graficaron las entidades con más ciberataques. Se nota un enfoque de ataques cibernéticos a la DIAN en donde supera el segundo puesto por casi 5 veces.

Dado este contexto, surge la siguiente pregunta de investigación: ¿Cuáles son los patrones y características comunes de las contraseñas en correos electrónicos que contribuyen a su debilidad y susceptibilidad a ataques?

2. MATERIALES Y MÉTODOS/METODOLOGÍA

La declaración PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), publicada en 2009, se diseñó para ayudar a los autores de revisiones sistemáticas a documentar de manera transparente el porqué de la revisión, qué hicieron los autores y qué encontraron (Page et al., 2021). En esta investigación, se siguió la metodología PRISMA adaptada al contexto de contraseñas débiles en correos electrónicos para obtener un panorama exhaustivo de la literatura y los estudios disponibles.

Las directrices PRISMA proporcionan recomendaciones detalladas para cada parte del proceso de revisión sistemática y requieren un escrutinio meticuloso de datos textuales extensos por parte de múltiples revisores lo que implica un esfuerzo humano considerable. (Landschaft et al., 2024).

.A continuación, se describen los pasos implementados bajo el esquema PRISMA:

1. Determinación de las fuentes de datos

El primer paso fundamental en el desarrollo de la metodología PRISMA consiste en seleccionar las bases de datos de las cuales se extraerán los estudios. Esta etapa se centra en asegurar que las fuentes sean reconocidas académicamente y que contengan investigaciones relevantes para la temática de estudio. Se decidió utilizar las siguientes bases de datos clave:

- **ScienceDirect:** Esta base de datos proporciona acceso a literatura científica revisada por pares en una amplia variedad de campos. Fue seleccionada por su reputación y su capacidad de proporcionar artículos relevantes sobre ciberseguridad, seguridad de contraseñas, y otras áreas críticas dentro de la seguridad informática.

- **Google Académico:** Aunque Google Académico no es tan específico como ScienceDirect, es una herramienta útil para acceder a una gran cantidad de literatura, incluidas tesis, artículos no indexados en otras bases de datos y documentos técnicos que tratan el tema de contraseñas vulnerables. Su alcance global también contribuye a capturar una mayor diversidad de estudios, lo que resulta valioso en una revisión exhaustiva.

- **JSTOR:** Esta base de datos ofrece acceso a revistas académicas, libros y fuentes primarias en diversas disciplinas. Se incluyó en la selección debido a su amplio contenido, que puede proporcionar perspectivas relevantes sobre el comportamiento de los usuarios respecto a la seguridad de contraseñas y vulnerabilidades en sistemas de información. Además, su cobertura histórica permite acceder a estudios importantes que podrían no estar presentes en otras bases de datos más recientes.

Estas fuentes fueron elegidas debido a su capacidad para ofrecer estudios de alta calidad que pudieran responder a las preguntas de investigación planteadas. Este proceso de selección de bases de datos forma una base sólida para asegurar la relevancia y rigor de los estudios incluidos en la revisión.

2. Definición de la estrategia de búsqueda

La estrategia de búsqueda es uno de los componentes más críticos en cualquier revisión sistemática, y su adecuada definición es clave para garantizar que se identifiquen todos los estudios relevantes. Siguiendo el enfoque PRISMA, se realizó una planificación que incluyó la definición de términos clave, la utilización de operadores booleanos, y el establecimiento de criterios para limitar los resultados a aquellos que sean más pertinentes.

Términos clave y combinaciones utilizadas:

- Contraseñas vulnerables
- Seguridad de la información
- Autenticación de usuarios
- Brechas de seguridad
- Ciberseguridad

2.1. Asesoramiento de expertos

Para afinar aún más la estrategia de búsqueda, se consultó con profesores y expertos vinculados con la Universidad Santiago de Cali. Este proceso fue valioso para identificar vacíos en la literatura y ajustar las búsquedas según las recomendaciones de los expertos, logrando así una recopilación más precisa y contextualizada de estudios relevantes.

3. Establecimiento de los criterios de inclusión y exclusión

La metodología PRISMA sitúa un fuerte énfasis en la rigurosidad y transparencia en la selección de estudios. Por ello, se definieron criterios claros de inclusión y exclusión para garantizar que solo se incluyan estudios de alta calidad y relevantes para el tema en cuestión.

Criterios de inclusión:

- Pertinencia temática: Se incluyeron estudios que examinarán aspectos más generales de la gestión de contraseñas en entornos corporativos, personales y casos de estudio.
- Rigor metodológico: Sólo se seleccionaron estudios que aplicaron metodologías robustas y claramente definidas.

Esto incluyó estudios empíricos, revisiones sistemáticas anteriores, y análisis cuantitativos sobre las prácticas de creación y gestión de contraseñas.

- Publicación reciente: Los estudios debían haber sido publicados en los últimos 10 años, asegurando así que los resultados fueran relevantes en el contexto actual de la ciberseguridad.

Criterios de exclusión:

- Estudios irrelevantes: Se excluyeron aquellos que no estaban directamente relacionados con el tema principal de contraseñas vulnerables o que no abordaban la cuestión de la seguridad en correos electrónicos.
- Población no representativa: Los estudios centrados en poblaciones que no fueran aplicables al contexto de nuestra investigación, o que no representaran adecuadamente el fenómeno de interés, fueron descartados.
- Estudios con sesgos significativos: Se eliminaron aquellos estudios que presentaban deficiencias metodológicas o sesgos importantes que pudieran comprometer la validez de los resultados.
- Duplicados: Al manejar múltiples bases de datos, fue esencial eliminar estudios duplicados que podrían haber aparecido en más de una fuente.

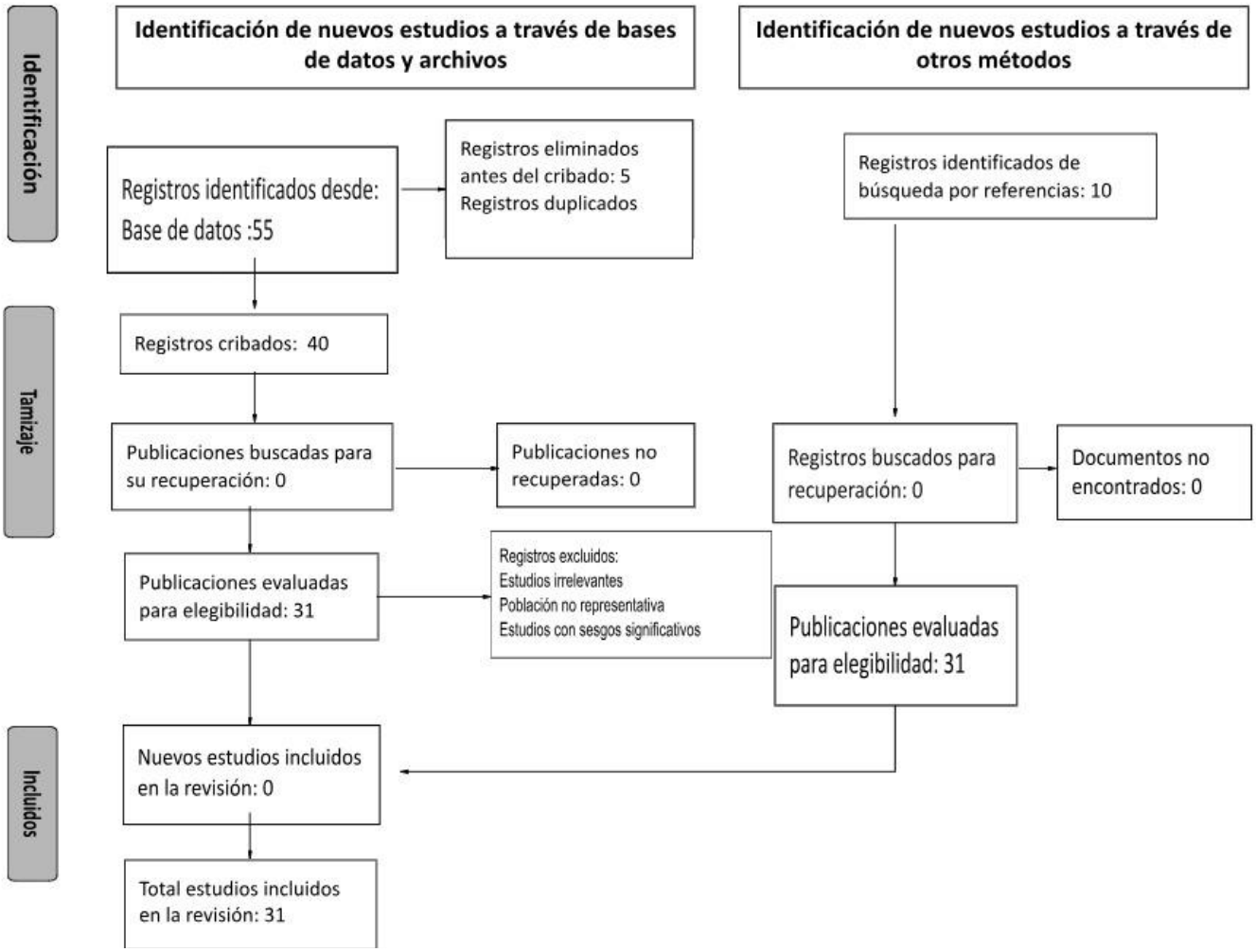
3.1 Ejemplos de exclusión adicional

Una gran parte de la investigación sobre contraseñas vulnerables se basa en contraseñas filtradas por atacantes. Estos conjuntos de datos, aunque útiles, suelen ser limitados en cuanto a información contextual, lo que impide obtener información detallada sobre cómo los usuarios crean contraseñas en función de sus antecedentes personales o culturales. Aquellos estudios que no proporcionaban este contexto adicional fueron excluidos del análisis.

4. Evaluación de la calidad de los estudios seleccionados

Siguiendo el enfoque PRISMA, una vez identificados los estudios relevantes, se aplicaron criterios adicionales para evaluar su calidad. Se utilizó una lista de verificación para garantizar que los estudios cumplieran con altos estándares de calidad en términos de diseño experimental, recolección de datos y análisis. Este paso fue fundamental para asegurar la fiabilidad y la validez de las conclusiones obtenidas a partir de la revisión.

Figura 1. Diagrama PRISMA de investigación documental.



Fuente: Elaboración propia, 2024.

3. RESULTADOS Y DISCUSIÓN

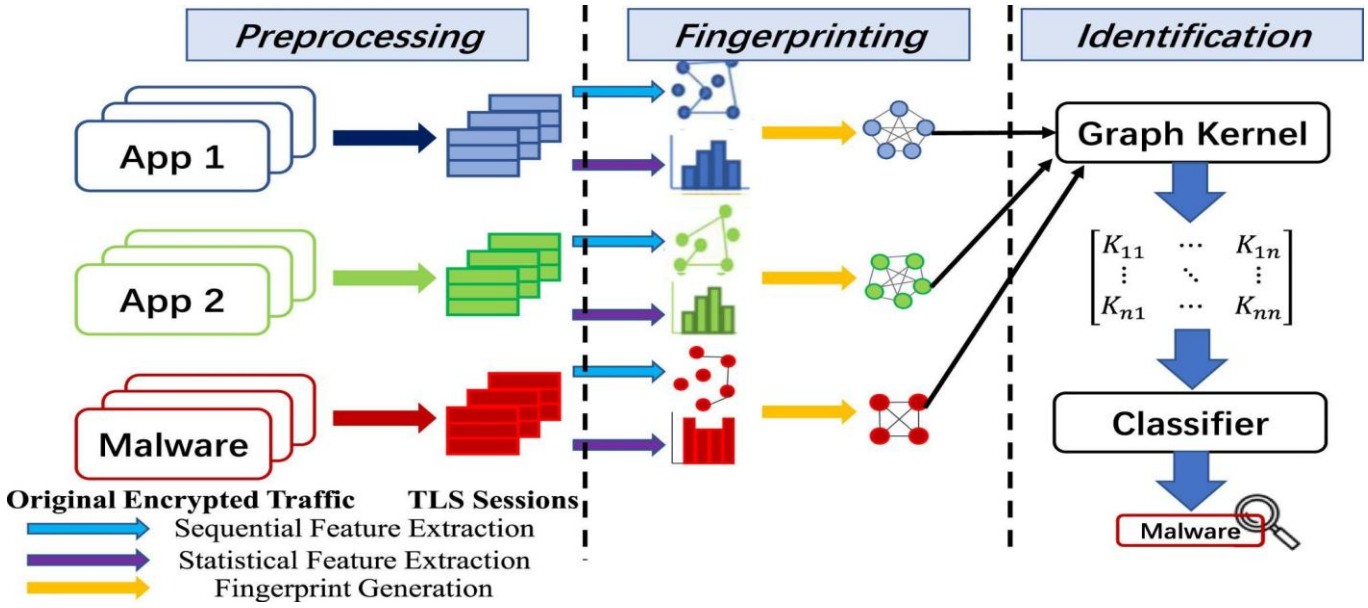
Ciberseguridad en protocolos de HTTPS

La implementación del protocolo HTTPS evidencia una carencia de estandarización que abarque todas las métricas críticas de seguridad. Esto se refleja en que, aunque el 54,17% de los métodos analizados incluye la "Redirección automática a HTTPS" como una medida esencial para mitigar las vulnerabilidades propias del uso de HTTP, solo el 41,67% evalúa la "Versión SSL/TLS" y apenas el 37,50% verifica la validez del certificado. Esto resalta la necesidad urgente de actualizar los protocolos de seguridad, asegurando el uso de versiones TLS más robustas y evitando certificados caducados (Zineddine et al., 2024).

En los correos electrónicos y en la mayoría de servicios de mensajería web se usa TLS (Yu et al., 2024). Para los ciberatacantes les es complicado acceder a la información de los usuarios debido a esta tecnología de cifrado, incrementando la seguridad, pero debido a la seguridad destacable, los atacantes la pueden usar a su favor, es decir, que los atacantes pueden enviar contenido malicioso cifrado, haciendo que la tarea de detectarlo sea casi imposible. Esto se debe a una alta complejidad computacional para desencriptar y plantea problemas en las políticas de privacidad para verificar la validez del certificado.

Debido a esta problemática, ya están surgiendo nuevas propuestas para contrarrestarlo, una de ellas es la formación de una huella digital TLS de la sesión. Combinan las huellas digitales de las sesiones, para obtener las huellas digitales de la aplicación correspondiente, permitiendo identificar el tráfico cifrado producido por el malware.

Figura 2. Descripción general de todo el proceso de identificación de tráfico malicioso cifrado.



Fuente: Yu et al., 2024.

La implementación de HTTPS muestra avances importantes en la protección de datos en línea, pero la falta de estandarización en métricas de seguridad clave limita su efectividad. La adopción desigual de prácticas como la redirección automática a HTTPS y la verificación de versiones SSL/TLS o de la validez de los certificados deja expuestas

brechas que pueden ser explotadas en un entorno de ciberamenazas en constante evolución. Aunque el cifrado TLS aumenta significativamente la privacidad en servicios de mensajería y correos electrónicos, también presenta desafíos, ya que los atacantes pueden aprovechar el cifrado para ocultar contenido malicioso. Para abordar esta problemática, las huellas digitales TLS de sesión ofrecen una herramienta prometedora, permitiendo identificar tráfico malicioso cifrado sin comprometer la privacidad del usuario.

El impacto del Phishing

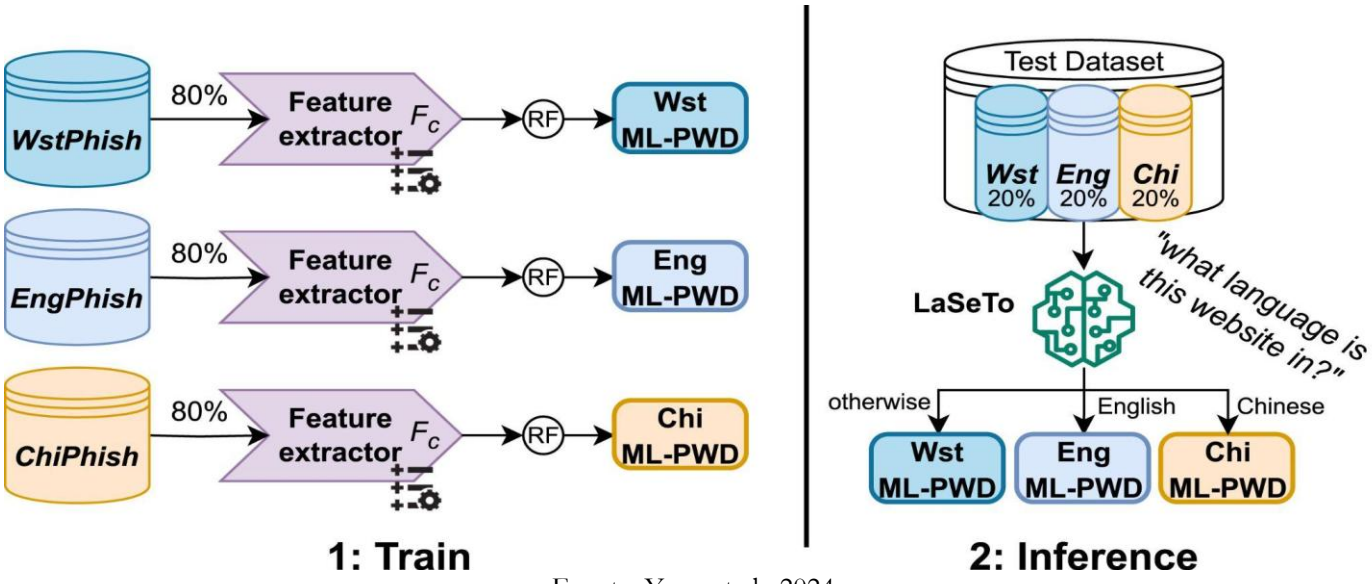
En este contexto, los correos electrónicos de phishing se convierten en una de las amenazas más extendidas para la ciberseguridad. Estos ataques aprovechan las vulnerabilidades humanas y el cifrado seguro para solicitar información confidencial o engañar a los usuarios para que accedan a enlaces maliciosos.

Los correos electrónicos de phishing intentan solicitar información confidencial y personal al atraer a los destinatarios para que hagan clic en archivos adjuntos o enlaces maliciosos dentro del correo electrónico; Además de comprometer la privacidad, los correos electrónicos de phishing pueden provocar pérdidas financieras sustanciales, interrupciones en el negocio y una reducción del bienestar de los empleados. En consecuencia, es necesario que los destinatarios de correo electrónico puedan identificar los correos electrónicos de phishing o tomar las medidas adecuadas para reducir su susceptibilidad a dichos correos electrónicos. (Sturman et al., 2024).

Los sistemas de detección de sitios web de phishing (PWD) actuales dependen en gran medida de listas de bloqueo estáticas, lo cual los hace vulnerables a amenazas sofisticadas y en constante evolución. Aunque se han desarrollado soluciones avanzadas basadas en aprendizaje automático (ML), estas se han centrado predominantemente en sitios web de países occidentales (idiomas como inglés, alemán o italiano), dejando de lado los sitios de países orientales, como China, donde el phishing es también una amenaza significativa (Yuan et al., 2024). Esta exclusión geográfica ha generado una brecha de efectividad en las PWD, evidenciada en tasas de detección notablemente bajas para sitios de phishing en chino, a veces inferiores al 1%.

Para enfrentar esta deficiencia, Yuan et al. (2024) desarrollaron CghPghrg, el primer conjunto de datos diseñado específicamente para evaluar PWD en sitios de phishing chinos, y llevaron a cabo una evaluación exhaustiva de 82 PWD (72 industriales y 10 basadas en ML). Con base en estos análisis, diseñaron un conjunto de características optimizadas que captura las particularidades de los sitios de phishing en chino, logrando así mejoras en la detección. Finalmente, integraron estos avances en un sistema PWD robusto capaz de detectar phishing en sitios de diversas regiones, alcanzando una tasa de detección superior al 98% y una tasa de falsos positivos de solo 0,01% en un entorno interregional.

Figura 3. Sistema de detección de sitios web de phishing basado en conjuntos.



Fuente: Yuan et al., 2024.

El phishing por correo electrónico es una de las amenazas más persistentes y dañinas en el ámbito de la ciberseguridad, explotando tanto las vulnerabilidades humanas como el cifrado para engañar a los usuarios y comprometer información confidencial. Los efectos de estos ataques van más allá de la pérdida de privacidad: pueden ocasionar pérdidas financieras significativas, interrupciones en las operaciones empresariales y un impacto negativo en el bienestar de los empleados. Esto resalta la importancia de que los usuarios desarrollen la habilidad de identificar intentos de phishing y adopten medidas para protegerse.

Sin embargo, los sistemas de detección actuales, que se basan principalmente en listas de bloqueo estáticas, son ineficaces ante las sofisticadas tácticas de phishing en constante evolución. A pesar del avance de los sistemas basados en aprendizaje automático, su alcance ha sido limitado geográficamente, dejando de lado amenazas en idiomas menos explorados, como el chino, donde el phishing también es un problema grave. Esta brecha de cobertura ha motivado el desarrollo de un nuevo conjunto de datos orientado a sitios de phishing en chino, mejorando la capacidad de los sistemas de detección para identificar amenazas de manera precisa y consistente en un entorno global. Este avance refuerza la necesidad de contar con soluciones interregionales robustas, capaces de adaptarse a un panorama de amenazas cada vez más global y diverso.

Contraseñas vulnerables en la seguridad informática

En un experimento estudiantil en la universidad de las Fuerzas Armadas de la ESPE en Ecuador en donde a los estudiantes hacen uso de un honeypot perteneciente a CEDIA, un puerto trampa que simula un servicio atractivo para los atacantes con el fin de registrar intentos de acceso no autorizado. para así usar contraseñas en diferentes sesiones para que cualquier persona en el mundo pudiera intentar hackearlo. Estas contraseñas fueron clasificados por dificultad como se ve en la siguiente tabla (Reyes et al., 2015):

Tabla 1. Clasificación de contraseñas por dificultad.

	No.	Alto	Medio	Bajo
Inglés	1	13ILÑPSSG@F	S0c4Cer3	Soccer1
	2	7TC@S@MBS5	F!0.w4er	Flower2
	3	5@GIG2MW@D	L0.vE_12	Lovel123
	4	&DTME*HP13	Ma!!f0.y	Malfoy2
	5	13G/GF*G/G	Ze4.us12	Zeus123
	6	5@*BCIS*@5	MaDr!d4	Madrid2
Español	7	13ILPSSG@F	Fut4b0!l	Futbol1
	8	7TC@S@MBS5	F!0.r4es	Flores2
	9	5@GIGG2MW@D	Am.0r_12	Amor123

Fuente: Reyes et al., 2015.

El experimento, que tuvo como objetivo evaluar la resistencia de diferentes niveles de complejidad de contraseñas frente a ataques automatizados, se llevó a cabo durante un mes utilizando una infraestructura de red académica. Los resultados obtenidos revelan que las contraseñas consideradas "Bajas" fueron las más vulnerables, recibiendo más del 50% de los intentos de ataque (Reyes et al., 2015). Este hallazgo confirma la importancia de utilizar contraseñas robustas y únicas para cada servicio en línea. Además, se observó una alta concentración de ataques provenientes de un reducido número de direcciones IP, lo que sugiere la existencia de botnets o grupos organizados dedicados a este tipo de actividades.

Tabla 2. Resultados de direcciones del atacante.

Nivel	Número de Ips	Número de sesiones	Número de Intentos
BAJO	225	69.359	204.188
MEDIO	139	13.289	35.449
ALTO	215	57.388	167.334

Fuente: Reyes et al., 2015.

Como resultado tuvieron 407.029 de todos estos se identificó que la gran mayoría (85%) provenían de China y Hong Kong. Este dato resulta particularmente revelador, ya que evidencia una concentración significativa de actividad maliciosa en estas regiones. En particular, se detectó una alta incidencia de ataques originados desde las redes de la empresa HEETHAI LIMITED, cuyas direcciones IP se encuentran en los rangos 103.41.124/25 y 103.41.125/25. Investigaciones posteriores permitieron establecer una conexión entre estas direcciones IP y el malware Massive DDoS Brute-Force Campaign Targets Linux Rootkits XOR.DDoS, el cual fue reportado por FireEye en septiembre de 2014 (Reyes et al., 2015). Este hallazgo sugiere que una parte considerable de los ataques recibidos formaban parte de una campaña de malware a gran escala con el objetivo de comprometer sistemas Linux.

Tabla 3. Intentos de ataques y su origen.

No	Ip	Ataques	Procedencia	Empresa registro
1	103.41.124.189	5917	China	HEETHAI LIMITED
2	103.41.124.123	4635	China	HEETHAI LIMITED
3	103.41.124.153	4382	China	HEETHAI LIMITED
4	43.255.190.188	4321	Hong Kong	SEXinSEX (Shimizu Hang Road)
5	103.41.125.17	3341	China	HEETHAI LIMITED

Fuente: Reyes et al., 2015.

Es crucial reconocer que este fenómeno no se limita a una geografía o sector específico; es una preocupación global. Los ciberdelincuentes operan a escala mundial, aprovechando cualquier oportunidad para infiltrarse y comprometer la seguridad digital.

Los resultados revelan una frecuencia alarmante de contraseñas débiles, reutilización común de contraseñas y un déficit en la longitud y complejidad de estas. Esta situación se traduce en un riesgo significativo de violaciones de seguridad, tanto a nivel individual como institucional. La persistencia de patrones predecibles en la creación de contraseñas agrava aún más la situación, facilitando el acceso no autorizado y los ataques de fuerza bruta.

El resultado del experimento en la universidad de las Fuerzas Armadas de la ESPE nos evidencia como buena propuesta para los usuarios que quieren acordarse de sus contraseñas de correos electrónicos el usar una contraseña de complejidad media, teniendo en cuenta que las aplicaciones web requieren aplicar medidas de seguridad cada vez más exigentes para evitar accesos no autorizados, lo que ha incrementado el grado de dificultad en el manejo de credenciales para los usuarios (Mena et al., 2021) y las contraseñas débiles permiten un fácil proceso de vulneración, ingresando a la cuenta de correo electrónico con facilidad.

La experiencia realizada en la Universidad de las Fuerzas Armadas de la ESPE, donde se implementó un honeypot para analizar el uso y efectividad de contraseñas en escenarios de acceso no autorizado, evidencia problemas recurrentes en la gestión de contraseñas que trascienden la geografía y sectores específicos, el fuerte de este estudio es claramente su cercanía con nuestro país Colombia y esto reafirmando la naturaleza global de esta amenaza. Los resultados obtenidos mostraron una preocupante recurrencia de contraseñas débiles y patrones predecibles, los cuales facilitan ataques de fuerza bruta y el acceso no autorizado a sistemas sensibles. Esta problemática refleja una carencia de prácticas adecuadas en la creación y administración de contraseñas, las cuales no solo representan un riesgo para los individuos, sino que también comprometen la seguridad de las instituciones. En este contexto, el uso de contraseñas de complejidad media surge como una alternativa viable para los usuarios que necesitan memorizar sus credenciales, aunque resulta insuficiente si no se acompaña de medidas de seguridad adicionales, como la autenticación multifactor. Este estudio subraya la necesidad de implementar políticas de seguridad que promuevan la creación de contraseñas robustas y únicas, considerando que el uso continuo de contraseñas débiles no solo facilita la vulneración de cuentas individuales, sino que también eleva el riesgo de comprometer información confidencial a nivel organizacional.

Predicción del próximo carácter en una contraseña basada en patrones de similitud

Han pasado más de 50 años desde que se introdujo y adoptó el concepto de contraseñas en nuestra sociedad como método de autenticación digital. A pesar de que posteriormente se desarrollaron métodos de autenticación alternativos, es razonable suponer que este método de autenticación predominante no perderá popularidad en un futuro próximo. (Kanta et al., 2022)

No obstante, el método Pwd Segment es una técnica de segmentación de contraseñas que busca dividir las contraseñas en fragmentos más pequeños llamados segmentos. Un fragmento es una subcadena que aparece frecuentemente en un conjunto de datos de contraseñas. Esta técnica optimiza el algoritmo Byte-Pair-Encoding (BPE) utilizando la longitud promedio personalizada de todos los fragmentos (avg_len) para sustituir el número de operaciones de fusión.

La técnica Pwd Segment consta de los siguientes pasos para segmentar y analizar contraseñas:

1. Segmentación de contraseñas (Pwd Segment): Se utiliza el método Pwd Segment para dividir contraseñas en fragmentos frecuentes, optimizando el algoritmo Byte-Pair-Encoding con un umbral de longitud promedio (avg len).

El proceso involucra la creación de un vocabulario de fragmentos, la segmentación iterativa de contraseñas, y la generación de secuencias de fragmentos.

2. Métodos de Incrustación de Palabras: Se emplean modelos de incrustación como Word2Vec, FastText y GloVe para convertir fragmentos en vectores de palabras, facilitando el cálculo de similitudes. Word 2 Vec y Fast Text consideran subpalabras para evitar problemas de vocabulario fuera de cobertura (OOV), mientras que GloVe utiliza una matriz de coocurrencia.

3. Calcular las probabilidades del siguiente carácter dentro de una contraseña: Las contraseñas de entrenamiento se segmentan y se generan nuevas reemplazando fragmentos con otros similares. Se seleccionan contraseñas comunes como semillas y se reemplazan fragmentos para crear un conjunto de adivinación.

4. Evaluación Experimental: Se utilizan conjuntos de datos filtrados (CSDN, Rockyou, Yandex) divididos en entrenamiento y prueba. Se analizan patrones y longitudes de contraseñas, observando que la mayoría son simples (letras o números puros) y de longitud 8-12 caracteres.

Tabla 4. Distribución de longitud de contraseñas por conjunto de datos.

DataSet	Lentght of passwords	Number of matched passwords	Percentage in dataset
CSDN	0-7 characters	57944	1.28%
	8-12 characters	4111257	91.14%
	13-20 characters	340799	7.56%
	over 20 characters	0	0%
Rockyou	0-7 characters	16172786	49.80%
	8-12 characters	15211672	46.85%
	13-20 characters	1093386	3.36%
	over 20 characters	32758	0.10%
Yandex	0-7 characters	563612	44.69%
	8-12 characters	634578	50.29
	13-20 characters	63616	5.04%
	over 20 characters	4	0.0003%

Fuente: Zhou et al., 2024.

El análisis de la técnica Pwd Segment para la segmentación de contraseñas pone en relieve el esfuerzo continuo por mejorar la seguridad de este método de autenticación a través de estrategias innovadoras. Aunque las contraseñas han sido predominantes durante más de 50 años y continúan siendo una solución ampliamente utilizada (Kanta et al., 2022), la segmentación de contraseñas en fragmentos frecuentes optimiza su resistencia frente a ataques. La técnica Pwd Segment, que emplea el algoritmo Byte-Pair-Encoding (BPE) ajustado por la longitud promedio de los fragmentos, permite la generación de secuencias más robustas y difíciles de predecir, manteniendo la facilidad de uso. Además, el uso de modelos de incrustación como Word2Vec, FastText y GloVe para representar estos fragmentos en vectores facilita la creación de similitudes entre contraseñas y la generación de nuevos intentos de adivinación mediante fragmentos similares. Los resultados experimentales, basados en conjuntos de datos conocidos como CSDN, Rockyou y Yandex, revelan patrones repetitivos y longitudes de contraseñas predominantemente simples, destacando que la mayoría de las credenciales analizadas siguen teniendo características predecibles, como el uso de letras y números únicamente. Este estudio resalta la importancia de seguir explorando métodos de segmentación y personalización para mejorar la seguridad de las contraseñas, destacando que aunque las contraseñas convencionales siguen siendo esenciales, los avances en técnicas como Pwd Segment representan una mejora sustancial frente a vulnerabilidades comunes en este tipo de autenticación.

Administración de contraseñas por usuarios

A pesar del crecimiento masivo de las herramientas de gestión de contraseñas, la memorización sigue siendo la técnica de seguimiento de contraseñas más común, y los administradores de contraseñas son ahora el segundo método más popular. Sorprendentemente, la introducción de llaves de seguridad físicas y claves de acceso de última generación ya ha atraído la atención y el 10% de su uso entre los adultos (Equipo de Security.org, 2023).

La creciente expansión de redes sociales y servicios de streaming impulsa a los usuarios a crear nuevas cuentas en diversas plataformas, lo cual a menudo requiere la creación y gestión de cuentas de correos electrónicos adicionales, incrementando la necesidad de contraseñas complejas que los usuarios deben gestionar. A pesar de esta oferta, un informe reciente reveló que el 41% de los usuarios aún depende de la memorización, y el 25% guarda las contraseñas en archivos no encriptados, los datos también indican un aumento en el uso de administradores de contraseñas, que subió del 20% al 34% de los adultos estadounidenses en un solo año (Equipo de Security.org, 2023). Esto evidencia la significativa vulnerabilidad ante ciberataques, como los 10.2 mil millones de dólares en cibercrimen reportados en el año 2022 por el FBI.

Tabla 5. Administración de contraseñas en línea.

¿Cómo administrar las contraseñas de tus cuentas en línea?	2022	2023
Tengo mis contraseñas memorizadas	41%	41%
Utilizo un administrador de contraseñas	21%	34%
Los escribo en papel	32%	30%
Guardo mis contraseñas en mi navegador	25%	27%
Los guardo en una nota en mi computadora o dispositivo móvil	25%	25%
Utilizo las mismas contraseñas en todas mi cuentas	22%	21%
Utilizo una clave de seguridad u otro dispositivio de contraseña física	-	10%

Fuente: Equipo de Security.org, 2023.

La adopción de bóvedas de contraseñas ha demostrado ser una solución efectiva para mitigar riesgos de seguridad asociados con la gestión y almacenamiento de credenciales. Al centralizar las contraseñas de los usuarios en un entorno seguro y cifrado, estas herramientas no sólo simplifican el proceso de autenticación, sino que también reducen la dependencia de prácticas riesgosas, como la repetición de contraseñas o el uso de combinaciones simples y predecibles. Gracias a la función de bóveda, los usuarios pueden acceder a credenciales seguras y complejas sin necesidad de recordarlas, mejorando la protección de sus cuentas frente a ataques de fuerza bruta y adivinación. Además, muchos administradores de contraseñas ahora integran el uso de claves de acceso y autenticación multifactor, brindando una capa adicional de seguridad al acceso de cuentas. Aunque el uso de bóvedas aún enfrenta desafíos, como la sincronización segura entre dispositivos y la protección de la contraseña maestra, su capacidad para gestionar contraseñas de manera eficiente y reducir las vulnerabilidades más comunes resalta su importancia en un entorno digital donde la complejidad y unicidad de las contraseñas son fundamentales para la seguridad.

Bóvedas de contraseñas

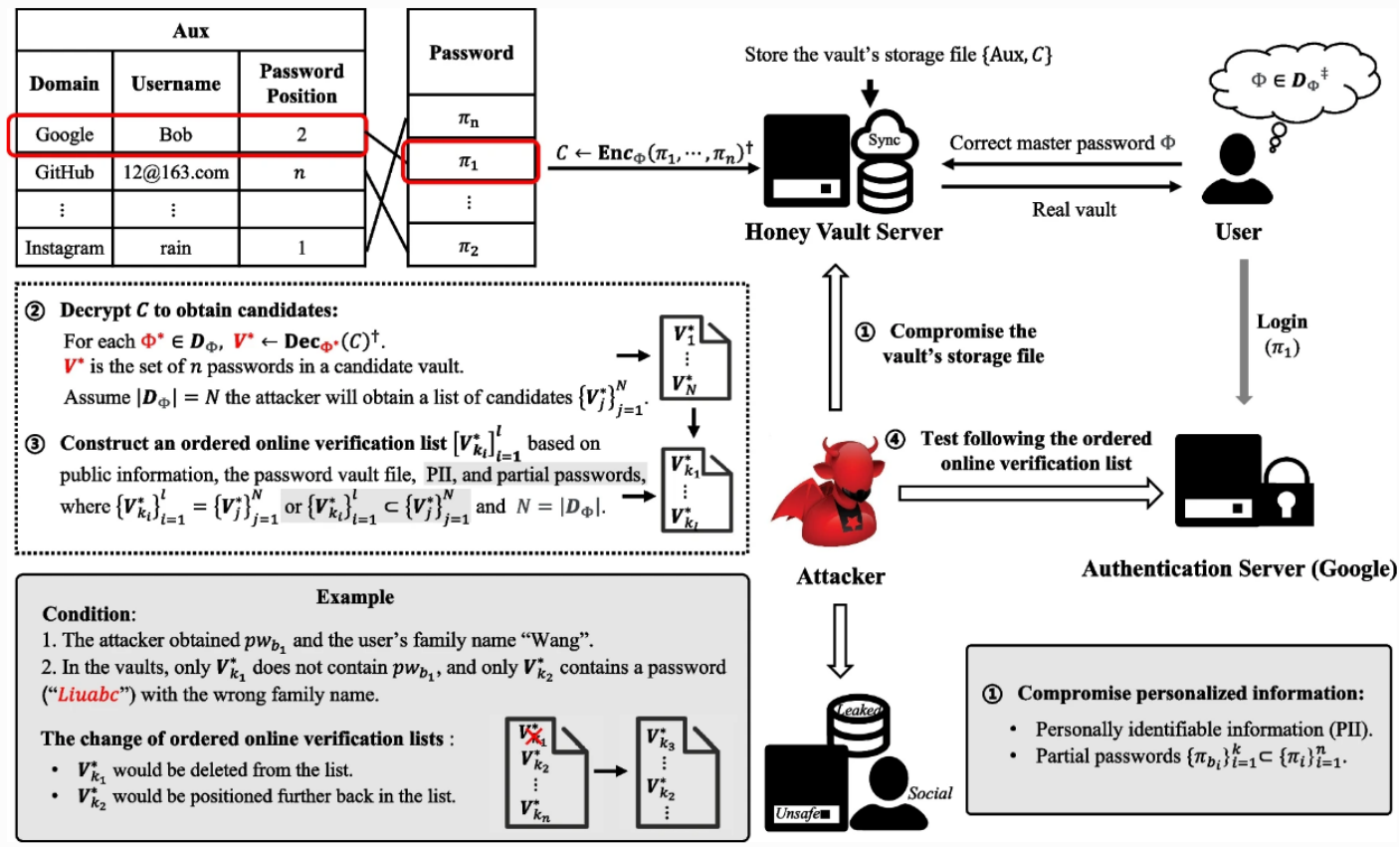
Las contraseñas siguen siendo el método de autenticación más utilizado debido a su practicidad. Sin embargo, los usuarios enfrentan el desafío de memorizar múltiples credenciales para distintos servicios y aplicaciones. Para facilitar esta tarea, surgieron las bóvedas o administradores de contraseñas, que almacenan las claves de forma cifrada y se protegen mediante una contraseña maestra definida por el usuario. En la práctica, es común que los usuarios deban sincronizar estas bóvedas entre varios dispositivos, como en el caso de iCloud Keychain. Sin embargo, los servicios de sincronización, tanto propios de aplicaciones como LastPass y 1Password, como de terceros, no están exentos de riesgos de filtración, incluso si los datos se encuentran cifrados (An et al., 2024).

Una alternativa prometedora para mitigar estos riesgos son las bóvedas Honey, que generan bóvedas señuelo cuando se introduce una contraseña maestra incorrecta. De este modo, los atacantes que acceden al archivo cifrado tienen dificultades para distinguir entre la bóveda legítima y las señuelo, sin realizar verificaciones en línea. No obstante, el mayor reto de estos sistemas es impedir que los atacantes identifiquen la bóveda real utilizando información filtrada, como contraseñas parciales o datos personales.

Los resultados experimentales obtenidos en el estudio permiten evaluar la efectividad del esquema de bóvedas Honey frente a ataques de contraseñas. Los ataques basados en información personal identificable (PII) logran distinguir la bóveda real de las señuelo en el esquema de Cheng et al. Este esquema se usa como punto de comparación dando una precisión del 63% al 70%. Sin embargo, en el esquema propuesto en este estudio, dicha precisión se reduce a un rango del 41% al 50%, acercándose al valor ideal del 50% en términos de incertidumbre del atacante. Este cambio implica que los atacantes necesitan realizar aproximadamente un 60% más de intentos para comprometer la bóveda real en comparación con el esquema de Cheng et al.

Además, se evalúa la seguridad contra ataques dirigidos específicamente a adivinar contraseñas parciales mediante PII. Un caso importante es en donde el atacante utiliza una lista de verificación en línea basada en ordenaciones de probabilidad. En este contexto, la efectividad del esquema es mayor, pues los ataques logran una precisión del 49%, lo que indica que la influencia de la PII en la seguridad de las contraseñas es limitada.

Figura 4. Propuesta del sistema de la bóveda de contraseñas Honey.



Fuente: An et al., 2024.

La dependencia de contraseñas como principal método de autenticación ha impulsado el uso de administradores de contraseñas o bóvedas, los cuales facilitan el almacenamiento cifrado y sincronización de credenciales entre dispositivos, como ocurre con iCloud Keychain o aplicaciones populares como LastPass y 1Password. Sin embargo, a pesar de sus ventajas, estos servicios no están exentos de riesgos, ya que la sincronización en múltiples dispositivos incrementa la vulnerabilidad frente a posibles filtraciones de datos, incluso en entornos cifrados (An et al., 2024). En respuesta a estos riesgos, las bóvedas Honey han surgido como una alternativa innovadora al generar bóvedas señuelo al introducir contraseñas maestras incorrectas. Esta estrategia complica el acceso no autorizado al forzar al atacante a distinguir entre bóvedas legítimas y falsas sin la certeza de haber accedido a la información real. A pesar de esta ventaja, el desafío central sigue siendo evitar que los atacantes identifiquen la bóveda genuina a través de información filtrada o el uso de datos personales conocidos. La implementación de las bóvedas Honey, aunque prometedora, subraya la necesidad de combinar múltiples estrategias de seguridad para maximizar la protección de credenciales, especialmente frente a actores que puedan emplear técnicas avanzadas de reconocimiento de patrones o verificación de datos.

4. CONCLUSIONES

En conclusión, los patrones y características comunes de las contraseñas en correos electrónicos que contribuyen a su debilidad y susceptibilidad a ataques incluyen la insuficiente longitud, la falta de caracteres especiales, la simplicidad en su composición y la reutilización en múltiples plataformas. Estos factores son explotados frecuentemente por atacantes a través de técnicas como ataques de diccionario, fuerza bruta y phishing.

El análisis de las debilidades comunes en contraseñas revela que la mayoría de las contraseñas vulnerables presentan patrones predecibles, como secuencias numéricas o palabras comunes, lo cual facilita los ataques de fuerza bruta al no

cumplir con los requisitos básicos de seguridad. Además, los factores que promueven estas malas prácticas incluyen la falta de conocimiento sobre la importancia de contraseñas seguras, la percepción de que la seguridad es secundaria frente a la conveniencia y la ausencia de políticas estrictas de gestión de contraseñas.

En entornos corporativos, estas contraseñas débiles representan un riesgo significativo, pueden ser la puerta de entrada a infraestructuras críticas y datos confidenciales, destacando la necesidad de implementar medidas de seguridad robustas, como la autenticación multifactorial y políticas de cambio de contraseñas periódicas. Aunque las técnicas de filtrado de contraseñas débiles han evolucionado, con mejoras como la integración de bases de datos de contraseñas comprometidas y el uso de algoritmos avanzados para generar contraseñas seguras, su adopción no es aún generalizada, dejando brechas significativas en la seguridad de la información.

Finalmente, se refuerza la necesidad de una colaboración activa entre usuarios y desarrolladores para fomentar una cultura de seguridad sólida, adoptando prácticas como el uso de gestores de contraseñas y la educación continua en ciberseguridad. Esto es fundamental para enfrentar las crecientes amenazas en el entorno digital actual y garantizar la integridad y confidencialidad de la información en las plataformas en línea.

5. REFERENCIAS

Aebischer, S., Dettoni, C., Jenkinson, G., Krol, K., Llewellyn-Jones, D., Masui, T., & Stajano, F. (2020). Deploying authentication in the wild: Towards greater ecological validity in security usability studies. Journal of Cybersecurity, 6(1), Article tyaa010. https://doi.org/10.1093/cybsec/tyaa010

Atzori, M., Calò, E., Caruccio, L., Cirillo, S., Polese, G., & Solimando, G. (2024). Evaluating password strength based on information spread on social networks: A combined approach relying on data reconstruction and generative models. Online Social Networks and Media, 42. https://doi.org/https://doi.org/10.1016/j.osnem.2024.100278

An, C., Xiao, Y., Liu, H., Wu, H., & Zhang, R. (2024). Honey password vaults tolerating leakage of both personally identifiable information and passwords. Cybersecurity, 7(1). https://doi.org/https://doi.org/10.1186/s42400-024-00236-6

Chhibbar, L. D., Patni, S., Todi, S., Bhatia, A., & Tiwari, K. (2024). Enhancing security through continuous biometric authentication using wearable sensors. Internet of Things, 28, 101374. https://doi.org/10.1016/j.iot.2024.101374

Equipo de Security.org. (2023). *Password manager annual report*. Security.org. https://www.security.org/digital-safety/password-manager-annual-report/

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. Scientific African, 21, e01743. https://doi.org/10.1016/j.sciaf.2023.e01743

Gaw, S., & Felton, E. (2019). Improving password memorability, while not inconveniencing the user. International Journal of Human-Computer Studies, 133, 26–44. https://doi.org/10.1016/j.ijhcs.2019.02.003

Kanta, A., Coisel, I., & Scanlon, M. (2022). A novel dictionary generation methodology for contextual-based password cracking. IEEE Access, 10, 59178-59188. https://doi.org/10.1109/ACCESS.2022.3179701

Kanta, S., Aikaterini, C., Sein, M., & Scanlon, M. (2021). How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts. Computers & Security, 107, 102366. https://doi.org/10.1016/j.cose.2021.102366

Landschaft, A., Antweiler, D., Mackay, S., Kugler, S., Rüping, S., Wrobel, S., Höres, T., & Allende-Cid, H. (2024). Implementation and evaluation of an additional GPT-4-based reviewer in PRISMA-based medical systematic literature reviews. International Journal of Medical Informatics, 189, 105531. https://doi.org/10.1016/j.ijmedinf.2024.105531

Maldonado Ortiz, F. B., Hernández, V. R., Salazar Hernández, R., & Llamas Mangin, M. Y. (2022). La paradoja de la seguridad informática durante la pandemia. ¿Son más vulnerables los alumnos de tecnologías de la información? [Artículo en línea]. Disponible en: http://www.dilemascontemporaneoseducacionpoliticayvalores.com/

Mena, V. P., & Gómez, O. S. (2021). Métodos de autenticación en aplicaciones web bajo un enfoque de usabilidad: Una revisión sistemática de literatura. RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação, 43, 467-483. https://www.researchgate.net/profile/Omar-S-Gomez/publication/353541241_Metodos_de_Autenticacion_en_Aplicaciones_Web_bajo_un_Enfoque_de_Usabilidad_Una_Revision_Sistematica_de_Literatura/links/610211331ca20f6f86e6088c/Metodos-de-Autenticacion-en-Aplicaciones-Web-bajo-un-Enfoque-de-Usabilidad-Una-Revision-Sistematica-de-Literatura.pdf

Mendivil Caldentey, J. S., Uglioli, B., & García, A. M. (2022). Formación y concienciación en ciberseguridad basada en competencias: Una revisión sistemática de literatura. Forensic Science International: Digital Investigation, 39, 301186. https://doi.org/10.1016/j.fsidi.2021.301186

Mendoza, A. G., Burgos, F. B., Sarmiento, C. C., & Rivas, W. R. S. (2020). La importancia de la autenticación multifactor para el usuario final en un entorno financiero. Informática y Sistemas: Revista de Tecnologías de la Información y las Comunicaciones. https://doi.org/10.33936/isrtic.v4i1.2347

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., Moher, D., Yepes-Nuñez, J. J., Urrútia, G., Romero-García, M., & Alonso-Fernández, S. (2021). Declaración PRISMA 2020: Una guía actualizada para la publicación de revisiones sistemáticas. Revista Española de Cardiología, 74(9), 790-799. https://doi.org/10.1016/j.recesp.2021.06.016

Reyes Ch, R. P., Dieste, O., & Fonseca C., E. R. (2015). El uso de contraseñas, un mundo lejos de la extinción: Un Estudio Empírico. https://doi.org/10.13140/RG.2.1.3545.0965

Sturman, D., Auton, J. C., & Morrison, B. W. (2024). Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses. *Computers & Security*, 104129. https://doi.org/10.1016/j.cose.2024.104129

Sunil, C., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50. https://doi.org/10.1016/j.cosrev.2023.100592

Valentina Castro. (2022). El riesgo de los ciberataques para Colombia. ESICI. Disponible en: https://esici.edu.co/wp-content/uploads/2023/04/Boletin-05-V5.pdf

Wang, J., Wang, G., Liu, J., & Wu, J. (2016). Continuous pyrolysis and catalytic upgrading of corncob hydrolysis residue in the combined system of auger reactor and downstream fixed-bed reactor. Energy Conversion and Management, 121, 137-144. https://doi.org/10.1016/j.enconman.2016.05.055

Wang, J., Wu, Z., Yuan, X., & Song, Z. (2024). Peer governance effects of information security breaches. Energy Economics, 129, 107264. https://doi.org/10.1016/j.eneco.2023.107264

Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab012

Woods, N., & Siponen, M. (2024). How memory anxiety can influence password security behavior. Computers and Security, 137. https://doi.org/10.1016/j.cose.2023.103589

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. Computers & Security, 133. https://doi.org/10.1016/j.cose.2023.103412

Yuan, Y., Apruzzese, G., & Conti, M. (2024). Beyond the west: Revealing and bridging the gap between Western and Chinese phishing website detection. Computers & Security, 104115. https://doi.org/https://doi.org/10.1016/j.cose.2024.104115

Yu, L., Tao, J., Xu, Y., Sun, W., & Wang, Z. (2024). TLS fingerprint for encrypted malicious traffic detection with attributed graph kernel. *Computer Networks*, *247*. https://doi.org/https://doi.org/10.1016/j.comnet.2024.110475

Zhou, E., Peng, Y., Shao, G., Deng, F., Miao, Y., & Fan, W. (2024). Password cracking using chunk similarity. *Future Generation Computer Systems, 150*, 380-394. https://doi.org/10.1016/j.future.2023.09.013

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer Studies, 133, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006

Zineddine, A., Chakir, O., Sadqi, Y., Maleh, Y., Singh Gaba, G., Gurtov, A., & Dev, K. (2024). A systematic review of cybersecurity assessment methods for HTTPS. Computers and Electrical Engineering, 115. https://doi.org/10.1016/j.compeleceng.2024.109137